

DISTRICT OF OREGON, ss: AFFIDAVIT OF HILARY A. RICKHER

**Affidavit in Support of an Application
Under Rule 41 for a Search Warrant**

I, Hilary A. Rickher, being duly sworn, do hereby depose and state as follows:

Introduction and Agent Background

1. I am a Special Agent with the U.S. Food and Drug Administration – Office of Criminal Investigations (FDA-OCI) and have been since September 2010. My current assignment includes conducting criminal investigations involving violations of the Federal Food, Drug and Cosmetics Act (21 U.S.C. §§ 301 et seq.) and other related federal crimes. Prior to my employment with FDA-OCI, I was a Postal Inspector with the United States Postal Inspection Service (USPIS), beginning in 2005. Prior to my employment with the USPIS, I was a Senior Patrol Agent with the United States Border Patrol, beginning in 2002. During my more than 17 years as a federal agent, I have conducted and/or participated in numerous criminal investigations involving violations of the federal mail fraud statute, drug and device distribution and importation violations, device adulteration violations, device misbranding violations, and other federal crimes. Specifically, I successfully completed the FDA-OCI Special Agent Training course in Charleston, South Carolina where I completed 120 hours of course work in FDA law and FDA-OCI investigations. I have also completed a 40-hour legal course regarding the Federal Food, Drug and Cosmetic Act. Additionally, I have participated in many aspects of drug investigations, including conducting physical surveillance, writing and executing search warrants, seizure warrants, and making arrests.

2. I submit this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search the premises located at [REDACTED]

[REDACTED] Portland, Oregon 97214 (hereinafter “Premises”), as described in

Attachment A hereto, for evidence, contraband, fruits, and instrumentalities of violations of 21 U.S.C. § 331(a) and (c). As set forth below, I have probable cause to believe that such property and items, as described in Attachment B hereto, including any digital devices or electronic storage media, are currently located at the Premises.

3. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter. The facts set forth in this affidavit are based on my own personal knowledge, knowledge obtained from other individuals during my participation in this investigation, including other law enforcement officers, interviews of witnesses, a review of records related to this investigation, communications with others who have knowledge of the events and circumstances described herein, and information gained through my training and experience.

Applicable Law

The Federal Food Drug and Cosmetic Act

4. The United States Food and Drug Administration (FDA) is the federal agency charged with the responsibility of protecting the health and safety of the American public by enforcing the Food, Drug and Cosmetic Act (FDCA), 21 U.S.C. § 301 et seq. Among the purposes of the FDCA is to ensure that medical products, including drugs, biologics, and devices, sold for consumption by or administration to humans, or for other use by or on humans, are safe, effective, bear labeling containing only true and accurate information, and have adequate directions for use. The FDA's responsibilities under the FDCA include regulating the manufacture, labeling, and distribution of all drugs, biologics, and medical devices shipped or received in interstate commerce.

5. Under the FDCA, the term “label” is defined as a display of written, printed, or graphic matter upon the immediate container of any article, including devices. 21 U.S.C. § 321(k). “Labeling” is a broader term, and is defined as all labels and other printed or graphic matter upon any article, including devices, or any of its containers or wrappers, or accompanying such articles. 21 U.S.C. § 321(m).

6. Under the FDCA, a “device” is, among other things, an instrument, apparatus, implement, machine, contrivance, implant, in vitro reagent, or other similar or related article intended for use in the diagnosis, cure, mitigation, treatment, or prevention of disease in man or other animals; or intended to affect the structure or any function of the body of man or other animals; and which does not achieve its primary intended purposes through chemical action within or on the body of man or other animals and which is not dependent upon being metabolized for the achievement of its primary intended purposes. 21 U.S.C. § 321(h).

7. Medical devices are classified into one of three categories, Class I, II, or III. Class III devices are those for which neither general nor special controls would provide a reasonable assurance of safety and effectiveness and those that are intended for use in supporting or sustaining life, are of substantial importance in preventing impairment of health, or present a potential unreasonable risk of illness or injury. 21 U.S.C. § 360c(a)(1)(C). Examples of Class III devices include pacemaker programmers, ventricular bypass devices, intraocular pressure measuring devices, and in vitro diagnostics, including antibody tests. 21 C.F.R. §§ 870.3700, 870.3545, 886.4280, 878.3540.

8. There is a second category of Class III devices. With the exception of certain devices that are exempt (by statute or regulation) from any premarket review, all "new" devices (those which were not in existence when the device amendments were passed in 1976) that come

on the market are automatically classified into Class III as a matter of law. 21 U.S.C.

§§ 360c(f)(1). In order to change that *de facto* status, a sponsor would need to obtain FDA's determination that the device can be marketed as a Class I or II device. In any circumstance, all non-exempt devices require either pre-market approval (PMA), clearance (via 510(k)), or the granting of a *de novo* application for reclassification by FDA before being marketed.¹

9. In vitro diagnostic products (IVDs) are those reagents, instruments, and systems intended for use in diagnosis of disease or other conditions, including a determination of the state of health, in order to cure, mitigate, treat, or prevent disease or its sequelae. Such products are intended for use in the collection, preparation, and examination of specimens taken from the human body. 21 C.F.R. § 809.3. IVDs are medical devices as defined at 21 U.S.C. § 321(h) and are subject to premarket and postmarket controls.

10. A prescription device is a device that, because of its potential for harmful effects, methods of use, or the collateral measures necessary to its use, is not safe for use except under the supervision of a practitioner licensed by law to direct the use of such device. 21 C.F.R. § 801.109.

11. Under the FDCA, a device is deemed to be misbranded unless its labeling bears adequate directions for use. 21 U.S.C. § 352(f)(1). In turn, "adequate directions for use" is defined as directions under which a layman can safely use a device for its intended uses. 21 C.F.R. § 801.5. By their very nature, prescription devices are safe for use only under the supervision of a licensed practitioner. 21 C.F.R. § 801.109. Because adequate directions for use cannot be written for prescription devices, they are misbranded under 21 U.S.C. § 352(f)(1).

¹ 21 U.S.C. § 360c(f)(2).

12. To allow for their lawful movement in interstate commerce, approved, cleared, or reclassified prescription devices are exempt from the adequate-directions-for-use requirement, but only if they meet certain conditions. See 21 C.F.R. § 801.109. One such condition requires that the device be in the possession of a person, or his agents or employees, regularly and lawfully engaged in the manufacture, transportation, storage, or wholesale or retail distribution of such device. 21 C.F.R. § 801.109(a)(1)(i).

13. Under the FDCA, a device is also misbranded if, among other things:

- its labeling is false or misleading in any particular way (21 U.S.C. 352(a));
- if its labeling fails to bear information required under the FDCA, and if this required information is not in the English language (21 U.S.C. § 352(c); 21 C.F.R. § 201.15(c)(1)); or
- the notice or other information respecting the device was not provided as required under section 510(k) of the FDCA (21 U.S.C § 360(k)) (21 U.S.C. § 352(o)).

14. A device is adulterated if, among other things, it is a Class III device, pursuant to 21 U.S.C. § 360c(f), was required under 21 U.S.C. § 360e(a) to have in effect an approved Pre-Market Application for Approval, and does not have such an approval in effect. 21 U.S.C § 351(f).

15. The doing or causing of the following acts are prohibited:

- The introduction into interstate commerce of an adulterated or misbranded device (21 U.S.C. § 331(a)); and

- The receipt in interstate commerce of devices that are misbranded or adulterated, and the delivery or proffered delivery thereof for pay or otherwise (21 U.S.C. § 331(c)).

16. Violations of 21 U.S.C. § 331 can be misdemeanors or felonies, depending on the circumstances. Violations done with an intent to defraud or to mislead consumers, regulators, or law enforcement are felonies. They carry a maximum penalty of up to three years in prison, and fines of up to \$250,000 for individuals or \$500,000 for corporations. If any person derives pecuniary gain from the offense, or if the offense results in pecuniary loss to a person other than the defendant, the defendant, whether an individual or a corporation, may be fined not more than the greater of twice the gross gain or twice the gross loss. 21 U.S.C. § 333(a); 18 U.S.C. § 3571.

Statement of Probable Cause²

17. In January 2020, the Secretary of Health and Human Services declared a public health emergency under section 319 of the Public Health Service Act (42 U.S.C. 247d), in response to SARS-CoV-2, more commonly known as COVID-19 and/or the Coronavirus (COVID-19). On March 13, 2020, the President of the United States declared a national

² Based on my training and experience, I use the following technical terms to convey the following meanings:

a. *Internet.* The Internet is a global network of digital devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

b. *Storage medium.* A storage medium is any physical object upon which data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

emergency to address the growing COVID-19 threat to our national security and well-being. On March 20, 2020, the U.S. Attorney for the District of Oregon, Billy J. Williams, issued a public statement to the media warning of the dangers of fraud schemes by those wishing to exploit the Coronavirus. U.S. Attorney William's press release was based on information provided by organizations such as the Federal Bureau of Investigation (FBI), the U.S. Federal Trade Commission (FTC) and InterPol. These scams include testing and treatment scams that utilize testing kits that are not cleared or approved by the FDA for use and may give false or unreliable results. As the FTC stated in their February 20, 2020, press release titled Scammer Follow the Headlines, "Scammers are taking advantage of fears surrounding the Coronavirus. They're setting up websites to sell bogus products, and using fake emails, texts, and social media posts as a ruse to take your money and get your personal information."

18. On February 4, 2020, the Secretary of Health and Human Services (HHS) determined that there was a public health emergency and that circumstances existed to justify the authorization of emergency use of in vitro diagnostics for detection and/or diagnosis of COVID-19. Rapid detection of COVID-19 cases in the United States required wide availability of diagnostic testing to control the emergence of this rapidly spreading, severe illness.

19. On February 29, 2020, the FDA issued a guidance, entitled "Policy for Diagnostic Tests for Coronavirus Disease -2019 during the Public Health Emergency, Immediately in Effect Guidance for Clinical Laboratories, Commercial Manufacturers, and Food and Drug Administration Staff, March 2020," describing a policy for laboratories and commercial manufacturers to help accelerate the use of tests they develop in order to achieve more rapid and widespread testing capacity in the United States. The guidance described two policies for accelerating the development of certain laboratory tests for COVID-19 – one leading to an

Emergency Use Authorization (EUA) submission to FDA, and the other not leading to an EUA submission when the test is developed under the authorities of the State in which the lab resides and the State takes responsibility for COVID-19 testing by laboratories in its State. In addition, this guidance described a policy for commercial manufacturers to more rapidly distribute their COVID-19 diagnostics to laboratories for specimen testing after validation while an EUA is being prepared for submission to FDA. Finally, this guidance also described a policy regarding the use of serological testing without an EUA. This guidance was updated on March 16, 2020. Notably, the emergency use guidance expressly excluded any home testing kits offered for direct sale to and use by consumers from the enforcement discretion articulated.

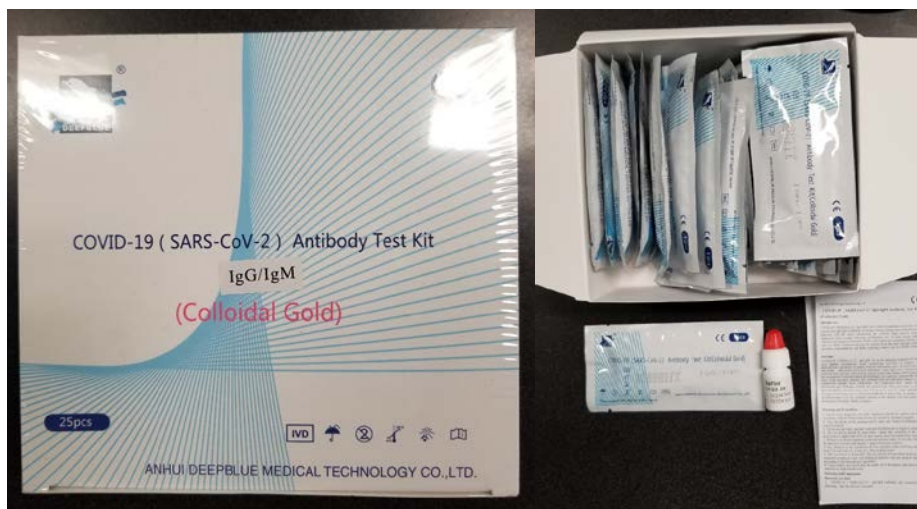
20. On March 18, 2020, U.S. Customs and Border Protection (CBP) Officer Hughes, exercising customs authorities, examined a package with air way bill (AWB) #510 2908 0501, which was manifested as “Papad (sic) Test Kit”, entering into the United States from China at the FedEx International Mail Facility in Memphis, Tennessee. Officer Hughes observed that the shipment contained four white boxes, each labeled as “COVID-19 (SARS-CoV-2) Antibody Test Kit (Colloidal Gold)”. Each box contained 25 individual kits, for a total of 100 test kits. Officer Hughes reviewed the shipment records and was unable to locate any FDA licenses having been filed with the shipment. After consultation with the FDA, the package was seized as an item prohibited from entering the United States. Below are photographs of the labeling of the product found in the parcel with AWB # 510 2908 0501:

///


///

///

///



21. The shipment labeled with AWB #510 2908 0501 showed a consignee of [REDACTED] at the Premises. An invoice that was seized as part of the shipping documents included in the package also listed the purchaser as [REDACTED] at the Premises.

 Anhui Deep Blue Medical Technology Co., Ltd Website: http://www.dbluemedical.com/ Address: 1#, D Zone, Four Floor, Pearl Industrial Park, 106 Innovation Avenue, Hefei Hi-tech Development Zone, Anhui					
Invoice					
To: [REDACTED]	Contract No: SLT2020031703				
Phone: [REDACTED]	Date: 2020/03/17				
Contact: [REDACTED]	Email: [REDACTED]				
Address: [REDACTED] Portland OR, 97217 [REDACTED]	Contact Person: [REDACTED]				
Item	Product	Weight(KG)	Qty (Tests)	Unit Price (USD)	Total Price (USD)
1	Rapid Test Kit (With Buffer) HS code: 3822001000 Packed in one carton	2kg	100	\$0.50	\$50.00

22. On March 20, 2020, Homeland Security Investigations (HSI) SA Glenn Dimmick conducted queries of law enforcement databases related to the seized shipment. A review of

Oregon Department of Motor Vehicles located records for [REDACTED] with Oregon driver's license [REDACTED] with an address of the Premises.

23. On March 20, 2020, Officer Oldham, with the Portland Police Bureau, conducted a physical address check of the Premises. Officer Oldham was unable to enter the building due to building access controls. However, Officer Oldham reviewed the publicly accessible tenant roster and observed that a [REDACTED] was listed as a tenant in the electronic call box.

24. On March 20, 2020, HSI SA Thomas Duffy reviewed the invoice included in package with AWB #510 2908 0501 and observed that the unit price was listed as \$.50 per unit with a total cost of \$50.00 for the 100 units. On March 23, 2020, SA Duffy spoke with a licensed medical doctor currently serving as the COVID-19 Physician Incident Commander for a major Portland, Oregon, area hospital. As the medical doctor explained, there are a wide variety of testing processes and costs can vary due to a litany of factors. However, the lowest level cost for a COVID-19 swab test is at least \$1,000 through certain private insurers and would require the use of an FDA-approved lab test center at additional costs. According to the COVID-19 Physician Incident Commander, "50 cents is ridiculous even for a swab. But for a test to actually give a result itself it's a preposterous cost."

25. On March 21, 2020, I reviewed the Oregon Medical Board online public license search, and [REDACTED] is not a licensed medical doctor in the state of Oregon. I also reviewed the Oregon State Board of Nursing online public license search, and [REDACTED] is not a registered nurse or nurse practitioner in the state of Oregon. I also reviewed the Oregon Board of Pharmacy online public license search, and [REDACTED] is not a licensed pharmacist or pharmacy in the state of Oregon.

26. On March 23, 2020, SA Duffy reviewed the State of Oregon's Secretary of State Corporate Division's public website. SA Duffy located a business registry for [REDACTED]. The articles of incorporation were filed on [REDACTED]. The article of incorporation lists [REDACTED] as the organizer, person with direct knowledge, and the registered agent. The articles list the Premises as the mailing address and as the principle place of business. SA Duffy conducted queries of law enforcement and public databases/websites and was unable to locate any website for [REDACTED] or find any type of information on [REDACTED] business activity. There is no type of business listed in the articles of incorporation or in the registry. Additionally, investigating agents have found no online presence of the company including a website, online reviews, or social media presence.

27. Previously, on March 20, 2020, SA Thomas Duffy reviewed the invoice included in the package with AWB #510 2908 0501 and observed that the phone number on the invoice was listed as [REDACTED]. SA Duffy conducted an open source internet search for the phone number and found that the area code [REDACTED] is used for the Houston, Texas, area. Additionally, SA Duffy was unable to locate any information showing that the phone number was linked to [REDACTED] or [REDACTED]. SA Duffy dialed phone number [REDACTED] from his government issued phone. SA Duffy noted that no one answered, and the call was directed to an automated voicemail box that did not indicate the name of the person or business that utilized the phone number. During SA Duffy's review of law enforcement databases related to [REDACTED], SA Duffy was not able to locate any records showing that [REDACTED] had ever resided in Texas. Further, [REDACTED] 2017 U.S. passport application listed a different personal phone number with a 503-area code. Based on my training and experience, legitimate businesses will use a call answering

service that list their name and general business information, such as business hours or a company directory.

28. On March 23, 2020, SA Duffy reviewed [REDACTED] public profile on the website LinkedIn. [REDACTED] listed that he was the Senior Vice-President of Supply Chain for [REDACTED] a cannabis oil company. SA Duffy reviewed the State of Oregon's Secretary of State Corporate Division's public website and found records that [REDACTED] was a registered company from [REDACTED] until the company failed to renew its business license in [REDACTED]. Law enforcement databases show that prior to his employment with [REDACTED] [REDACTED] was employed at a car dealership.

29. SA Duffy reviewed Department of Homeland Security (DHS) databases for items being imported to the Premises. DHS records show that since January 1, 2020, [REDACTED] was the consignee for the only two other packages being imported to that address. Both of those shipments occurred in January 2020 and were listed as clothes, which were shipped from a different company than the company that shipped the package with AWB #510 2908 0501.

30. On March 23, 2020, SA Duffy conducted a physical address check of the Premises. SA Duffy entered the lobby and observed that the address was a residential apartment building. SA Duffy observed that [REDACTED] appeared to be a residential address. SA Duffy noted that there were no signs or indicators that [REDACTED] housed a business, particularly, [REDACTED].

31. I have reviewed the labeling of the product found in the parcel with AWB #510 2908 0501. The labeling for "COVID-19 (SARS-CoV-2) Antibody Test Kit (Colloidal Gold)" lists Anhui DeepBlue Medical Technology Co. Ltd of Hebei, China, as the manufacturer. I have

reviewed the public online database for approved and cleared medical devices, and there is no record that this medical device is approved or cleared by the FDA.

32. I reviewed the package insert that accompanied the medical devices. The intended use is listed as, “COVID-19 (SARS-CoV-2) 1gG/1gM Test is used for qualitative detection of novel coronavirus 1gG/1gM antibodies in human serum, plasma and whole blood. After injection with the novel coronavirus...” In further examination of the package insert, there are various spelling and grammatical errors in the document.

33. I reviewed the Twitter account for Chin Xinhau News and saw the product with similar labeling as the product previously described. Although the labeling in the tweet is in Chinese, the labeling has the same logo as the product at issue, in the upper right corner of the box with a dolphin and the name, “DeepBlue.” The tweet states, “15 minutes! New rapid test strips for #coronavirus have been developed by a company in Hefei, China. #FightVirus.” The video in the tweet depicts a draw of blood from a finger pin prick. The drop of blood is then placed on a test strip.



The video states, “[t]he test strip has been proven to be effective after clinical tests.” The video further states, “[t]he company said the test strip may be available on the Chinese market soon.”

The comments on this tweet indicate the test kits efficacy is not known and unproven:



I know from my training and experience that marketers of unapproved products take advantage of vulnerable patients with promises that are unfounded.

34. On March 23, 2020, I requested a review of the product and labeling by FDA’s Center for Devices and Radiological Health (CDRH), the entity that regulates, approves, and clears medical devices. Dr. Leroy Hwang, Ph.D., Lead Consumer Safety Officer, Division of Microbiology Devices, CDRH, FDA, stated, “The test kits in the photos do NOT (his emphasis) have PMA or 510(k) clearance.”

35. I asked Dr. Hwang to describe, for background, how a legitimate antibody test kit works, as the product at issue is labeled, in part, “Antibody Test Kit.” Dr. Hwang responded, “These tests are for the detection of human antibody response (IgG/IgM) to the COVID-19 virus. The antibody test kits are often used to identify if an individual has circulating antibodies against a pathogen, which can be an indicator of either active (IgM) or previous (IgG) infection

by the pathogen. However, in the case of COVID-19 virus, it has yet to be established what correlation there is between different antibody levels and infection status of the individual.”

36. Dr. Hwang confirmed that the test kits labeled, “COVID-19 (SARS-CoV-2) Antibody Test Kit (Colloidal Gold)” do not have PMA or clearance. These types of devices would require one or the other. Therefore, the test kits are unapproved/uncleared medical devices. However, in light of the pandemic, the FDA has issued the previously described guidance document. The guidance document discusses that circumstances exist justifying the authorization of emergency use of in vitro diagnostics for detection and/or diagnosis of COVID-19. Dr. Hwang stated these test kits could possibly fall under the emergency use authorization (EUA). Dr. Hwang provided me with a copy of the guidance document, which states in pertinent part, “The policy...applies to commercial manufacturers that seek to develop and distribute diagnostic test kits to detect the SARS-CoV-2 virus to clinical laboratories or to healthcare workers for point-of-care testing. This policy does not apply to at home testing.” Dr. Hwang further stated, “There are currently no approved, cleared, or EUA authorized COVID-19 test kits for at-home use. If these kits are marketed for home use or distributed for home use, they are in violation, as the current Coronavirus IVD EUA guidance explicitly states that the policies allowing distribution without an EUA does NOT (his emphasis) apply to at home testing.” A review law enforcement, business registry, and FDA databases shows no record of [REDACTED] owning, operating, or acting in any capacity as a manufacturer of medical products.

37. Additionally, they lack adequate directions for use by a lay person, in that the test kits are prescription medical devices and require the expertise of medical practitioner to

administer the test, interpret the results, and importantly, provide the treatment to the tested subject. As such, the test kits are misbranded.

38. Dr. Hwang further stated, “At home testing use of non-EUA serology tests have potential for public health risk. If a test provides a false-negative result, an infected individual may be a risk to expose others to the disease. If a test provides a false-positive result, the individual may take actions that may cause additional burden on the healthcare system of handling a non-COVID-19 individual as being potentially infected and also may pose a risk to exposure events to themselves if they are quarantined with infected individuals due to the incorrect false positive test result.”

39. As previously stated, [REDACTED] is not a licensed medical professional, nor is there any indication he owns, operates or is employed by a clinical lab. In addition, Dr. Hwang told me that he found no record of [REDACTED] registering with the FDA.

40. Dr. Hwang verified that Anhui DeepBlue Medical Technology Co., Ltd. of Hefei, China, is registered with the FDA as a “Contract Manufacturer; Manufacturer.” To his knowledge, the company does not hold any PMA or cleared devices.

41. I have also reviewed the Clinical Laboratory Improvement Amendments (CLIA) Laboratory Search tool and found no record of any CLIA certified labs at the Premises. CLIA are federal regulatory standards that apply to all clinical laboratory testing performed on humans in the United States. CLIA Program sets standards and issues certificates for clinical laboratory testing. CLIA defines a clinical laboratory as any facility which performs laboratory testing on specimens derived from humans for the purpose of providing information for the diagnosis, prevention, or treatment of disease. An objective of the CLIA is to ensure the accuracy, reliability and timeliness of test results regardless of where the test was performed.

42. As described above and in Attachment B, this application seeks permission to search for records that might be found on the Premises, in whatever form they are found. One form in which the records will likely be found is data stored on a computer's hard drive, on other storage media, or other digital devices, including cell phones (hereinafter collectively referred to as digital devices). Thus, the warrant applied for would authorize the seizure of electronic storage media or the copying of electronically stored information, all under Rule 41(e)(2)(B).

43. There is probable cause to believe, and I do believe, that records will be stored on a digital device because, based on my knowledge, training, and experience, I know:

a. Computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a digital device, deleted, or viewed via the Internet. Electronic files downloaded to a digital device can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. When a person "deletes" a file on a digital device, the data contained in the file does not actually disappear; rather, that data remains on the digital device until it is overwritten by new data. Therefore, deleted files or remnants of deleted files, may reside in free space or slack space—that is, in space on the digital device that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a digital device's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

b. Wholly apart from user-generated files, digital devices—in particular, internal hard drives—contain electronic evidence of how a digital device has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating

system or application operation, file system data structures, and virtual memory “swap” or paging files. Digital device users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

c. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or “cache.”

d. I know individuals use their digital devices to search for and purchase items, including prohibited items and contraband. On March 23, 2020, I searched for Anhui DeepBlue Medical COVID-19 test kits and found they were available online at dblumedical.com. In addition, Anhui DeepBlue Medical has a storefront at the ecommerce website Alibaba.com. Purchases can be made from these websites using a smartphone, tablet or computer with internet access. Based on the facts of this investigation, specifically that these test kits are available online and were shipped from China, I am aware that digital devices were likely used to generate, store, and print documents used in the purchase of misbranded medical devices. Thus, there is reason to believe that there is a digital device currently located on the Premises.

44. As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant but also for forensic electronic evidence that establishes how digital devices were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any digital device in the Premises, because, based on my knowledge, training, and experience, I know:

a. Data on the digital device can provide evidence of a file that was once on the digital device but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, email programs, and chat programs store configuration information on the digital device that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the digital device was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created.

b. Forensic evidence on a digital device can also indicate who has used or controlled it. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. For example, registry information, configuration files, user profiles, email, email address books, “chat,” instant messaging logs, photographs, the presence or absence of malware, and correspondence (and the data associated with the foregoing, such as file creation and last-accessed dates) may be evidence of who used or controlled the digital device at a relevant time. Further, forensic evidence on a digital device can show how and when it was accessed or used. Such “timeline” information allows the forensic analyst and investigators to understand the chronological context of access to the digital device, its use, and events relating to the offense under investigation. This “timeline” information may tend to either inculcate or exculpate the user of the digital device. Last, forensic evidence on a digital device may

provide relevant insight into the user's state of mind as it relates to the offense under investigation. For example, information on a digital device may indicate the user's motive and intent to commit a crime (e.g., relevant web searches occurring before a crime indicating a plan to commit the same), consciousness of guilt (e.g., running a "wiping program" to destroy evidence on the digital device or password protecting or encrypting such evidence in an effort to conceal it from law enforcement), or knowledge that certain information is stored on a digital device (e.g., logs indicating that the incriminating information was accessed with a particular program).

c. A person with appropriate familiarity with how a digital device works can, after examining this forensic evidence in its proper context, draw conclusions about how digital devices were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a digital device that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a digital device is evidence may depend on other information stored on the digital device and the application of knowledge about how a digital device behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a digital device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a digital device. For example, the presence or absence of counter-

forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

45. In most cases, a thorough search of the Premises for information that might be stored on a digital device often requires the seizure of the device and a later, off-site review consistent with the warrant. In lieu of removing a digital device from the Premises, it is sometimes possible to image or copy it. Generally speaking, imaging is the taking of a complete electronic picture of the digital device's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the digital device and to prevent the loss of the data either from accidental or intentional destruction. This is true because:

a. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a digital device has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine digital devices to obtain evidence. Digital devices can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

b. Records sought under this warrant could be stored in a variety of formats that may require off-site reviewing with specialized forensic tools. Similarly, digital devices can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them

sometimes requires tools or knowledge that might not be present on the search site. The vast array of hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the Premises. However, taking the digital device off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

46. *Nature of the examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant for which I apply would permit seizing, imaging, or otherwise copying digital devices that reasonably appear to contain some or all of the evidence described in the warrant and would authorize a later review of the device or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire device, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

47. The initial examination of the digital device will be performed within a reasonable amount of time not to exceed 120 days from the date of execution of the warrant. If the government needs additional time to conduct this review, it may seek an extension of the time period from the Court within the original 120-day period from the date of execution of the warrant. The government shall complete this review within 180 days of the date of execution of the warrant. If the government needs additional time to complete this review, it may seek an extension of the time period from the Court.

48. If, at the conclusion of the examination, law enforcement personnel determine that particular files or file folders on the digital device do not contain any data falling within the scope of the warrant, they will not search or examine those files or folders further without authorization from the Court. Law enforcement personnel may continue to examine files or data

falling within the purview of the warrant, as well as data within the operating system, file system, software application, etc., relating to files or data that fall within the scope of the warrant, through the conclusion of the case.

49. If an examination is conducted, and the digital device does not contain any data falling within the ambit of the warrant, the government will return the digital device to its owner within a reasonable period of time following the search and will seal any image of the digital device, absent further authorization from the Court.

50. The government may retain the digital device as evidence, fruits, contraband, or an instrumentality of a crime or to commence forfeiture proceedings against the digital device and/or the data contained therein.

51. The government will retain a forensic image of the digital device for a number of reasons, including proving the authenticity of evidence to be used at trial, responding to questions regarding the corruption of data, establishing the chain of custody of data, refuting claims of fabricating, tampering, or destroying data, and addressing potential exculpatory evidence claims where, for example, a defendant claims that the government avoided its obligations by destroying data or returning it to a third party.

Conclusion

52. Based on the foregoing, I have probable cause to believe that [REDACTED] committed the unlawful act of the introduction into interstate commerce a misbranded device and received in interstate commerce a misbranded medical device in violation of 21 U.S.C. § 331(a) and (c) and that evidence of those offenses, as described above and in Attachment B hereto, are presently located at the Premises, which is described above and in Attachment A hereto. I therefore request that the Court issue a warrant authorizing a search of the Premises described in

Attachment A for the items listed in Attachment B and the seizure and examination of any such items found.


53. Prior to being submitted to the Court, this affidavit, the accompanying application, and the requested search warrant were all reviewed by Assistant United States Attorney (AUSA) Scott E. Bradford, and AUSA Bradford advised me that in his opinion the affidavit and application are legally and factually sufficient to establish probable cause to support the issuance of the requested warrant.

Request for Sealing

54. It is respectfully requested that the Court issue an order sealing, until further order of the Court, all papers submitted in support of the requested search warrant, including the application, this affidavit, the attachments, and the requested search warrant. I believe that sealing these documents is necessary because the information to be seized is relevant to an ongoing investigation, and any disclosure of the information at this time may result in the tampering of evidence or otherwise seriously jeopardize the investigation. Premature disclosure of the contents of the application, this affidavit, the attachments, and the requested search warrant may adversely affect the integrity of the investigation.

By phone
 Hilary A. Rickher
 Special Agent
 US Food and Drug Administration –
 Office of Criminal Investigations

Sworn in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone at
9:38 a.m on March 25, 2020.


 HONORABLE YOULEE YIM YOU
 United States Magistrate Judge